Privacy Act 102
Safeguarding Privacy Act Data

Mandatory Training for All Employees, Military Members, and Contractors

Why You Are Being Asked to Take this Training Now

- **In a number of recent incidents, personal data has been lost, stolen, or compromised. The most recent theft occurred when a Federal employee took home data on 26.5 million veterans in violation of Department of Veterans Affairs policy.**

- **The Office of Management and Budget, the Federal entity responsible for overseeing the Privacy Act, has mandated that the Federal workforce complete this training by June 22, 2006.**

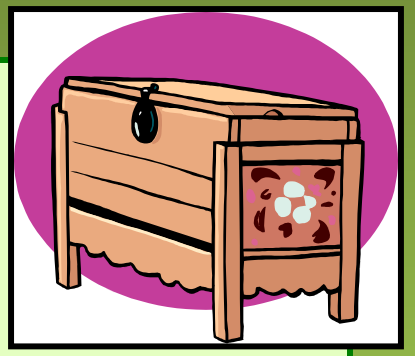
- **We don't want you to be the next accused of carelessly handling personal data!**

What is Privacy Act Data?

Definition

Any item of information about an individual (i.e., educational history, personnel data, employment history, financial transactions, medical information, criminal history, etc.) that is (1) maintained by an Agency and (2) is identifiable to that individual.

Safeguarding Requirements



- **Three Levels of Safeguards are Required:**
  - **Administrative**
  - **Physical**
  - **Technical**

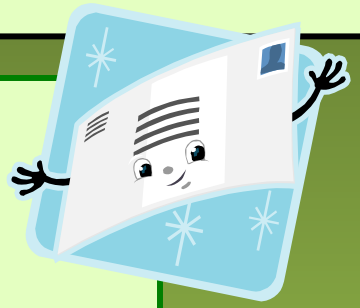
- **These individuals are responsible for establishing safeguards:**
  - **Information Technology System Designers**
  - **Privacy Act System Managers**
  - **Local Privacy Act Officials**

- **These individuals are responsible for seeing that safeguards are applied:**
  - **YOU!**

Marking Privacy Data

- **Before disseminating Privacy Act data, make sure it is marked to alert the receiver as to the sensitivity of the information.**
- **Reflect "FOUO" in message traffic that contains personal data.**
- **Emails and paper records should be marked. For example: "For Official Use Only – Privacy Sensitive – Any misuse or unauthorized disclosure may result in both civil or criminal penalties."**

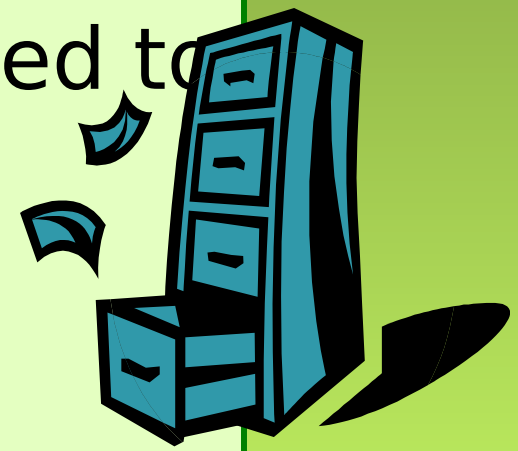
Transporting Privacy Data



- **Using Ground Mail:**
  - **Never use “holey joes” or messenger-type envelopes.**
  - **You may double wrap using an inner and outer envelope if you deem if appropriate.**
  - **Mark the envelope to the attention of an authorized recipient.**
  - **Never indicate on the outer envelope that it contains Privacy Data.**
- **Using E-mail:**
  - **Use Common Access Card procedures.**
  - **Announce in the opening line of text that you are relaying FOUO material.**

Storing Privacy Data

- Don’t leave privacy data in the open for anyone to view.
- Ensure information is not accessible to individuals that do not have an official need to know.
- Don’t store it in a public folder.



Disposing of Privacy Data

- **Use any means that prevents inadvertent compromise. A disposal method is considered adequate if it renders the information unrecognizable or beyond reconstruction.**

- **Disposal methods may include:**
  - **Tearing**
  - **Burning**
  - **Melting**
  - **Chemical decomposition**
  - **Pulping**
  - **Pulverizing**
  - **Shredding**
  - **Mutilation**

Sharing Privacy Act Data

- **Follow the “need-to-know” principle. Share only with those specific DoD employees who need the data to perform official, assigned duties.**

- **If you have doubts about sharing data, consult with your supervisor, the Privacy Act system manager, or your local Privacy Act Officer.**

Information for Teleworkers

- **Paper Records**
  - **Place Privacy Act data in locked drawers, locked briefcases, or other secure areas where family or household members cannot access it**
- **Electronic Records**
  - **Use password protection protocols. Share your password with no one.**
- **Don’t Dispose in Regular Trash**

Reporting Inappropriate Disclosures

- **Immediately notify your supervisor, your local Privacy Act Officer, the Privacy Act System Manager, or any other appropriate official of the occurrence.**

- **For World Wide Web postings, make a note of where the information was posted by copying the Uniform Resource Locator (URL). The URL is the address listed at the top of the screen. Most URLs begin http://www.**

Criminal Penalties for Noncompliance with the Privacy Act

- **For knowingly and willfully disclosing Privacy Act data to any person not entitled to access:**
  - **Misdemeanor criminal charge, and a fine of up to $5000.**
- **For maintaining a System of Records without meeting the public notice requirements:**
  - **Misdemeanor criminal charge, and a fine of up to $5000.**
- **For knowingly and willfully requesting or obtaining records under false pretenses:**
  - **Misdemeanor criminal charge, and a fine of up to $5000.**

Civil Penalties for Noncompliance with the Privacy Act

- **The Privacy Act also imposes civil penalties on violators who:**
  - **Unlawfully refuse to amend a record**
  - **Unlawfully refuse to grant access to records**
  - **Fail to maintain accurate, relevant, timely and complete data**
  - **Fail to comply with any Privacy Act provision or agency rule that results in an adverse effect.**
- **Penalties include:**
  - **Payment of actual damages**
  - **Payment of reasonable attorney's fees**
  - **Removal from employment**

If You Have Access to Personal Data . . .

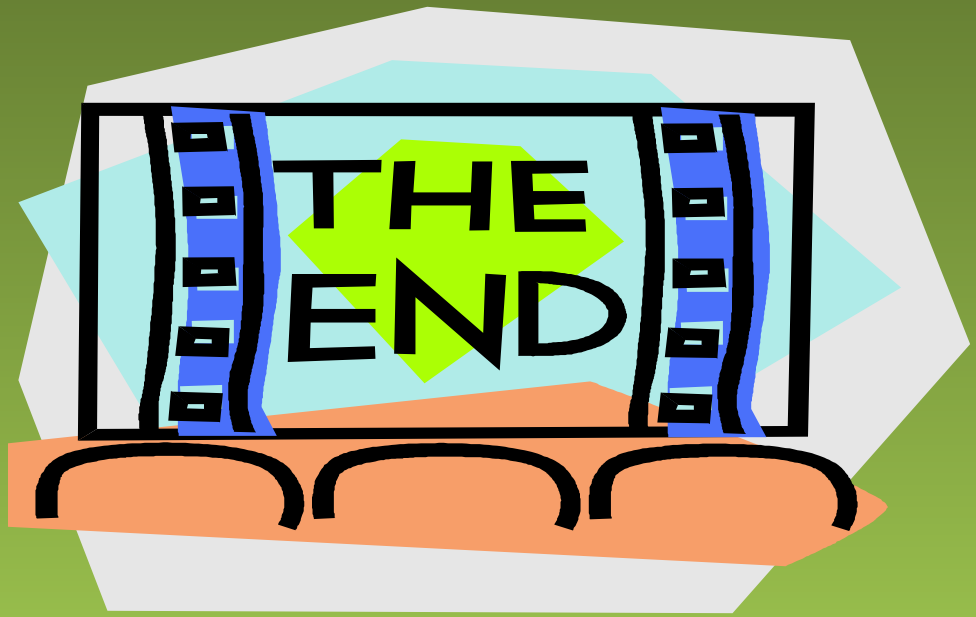
- **Protect it at all times.**
- **Limit access to those individuals who have an official need to know inside the agency and for those outside the agency access must be permitted under the conditions of disclosure in Section (b) of the Privacy Act or**
  - **The record subject has given you written permission to disclose it.**
- **Password protect personal data placed on shared drives, the Internet or the Intranet.**
- **Monitor your actions: If I do this, will I increase the risk of unauthorized access?**

Remember:

You may be subject to civil and criminal penalties for violating the Privacy Act.

More Tips for Avoiding Privacy Breaches

- **Take privacy protection seriously.**
- **Respect the privacy of others.**
- **Alert your supervisor or other management official when you see personal data left unattended.**
- **Know the Privacy Act requirements.**



Thank you for completing this important training!